Amendments to the Drawings:

The attached replacement sheets of drawings, includes changes to Fig. 1, 2 and 3 and replaces the original sheet including Fig. 1, 2 and 3

In Figure 1 the reference line for "operator console 16" was moved to point to the edge of the network.

In Figure 2 reference lines for "collectors" were provide with double arrow ends and arrows were added to reference designations 15a and 15b.

In Figure 3 the reference designation for "memory" was changed from "34" to –32-- and the designation for "storage" was changed from "36" to –34--.

Attachments following last page of this Amendment:

Replacement Sheet (3 pages)

## REMARKS

### Drawings Objection

The Examiner objected to Applicant's Figures 1-3. Applicant has enclosed herewith replacement sheets for FIGS. 1-3 and changes to the specification to overcome this objection. No new matter has been added.

### 35 U.S.C. 102

The Examiner rejected claims 8, 9, 11-13, 15, 16 and 18-21 under 35 U.S.C. 102(e), as being anticipated by US Patent publication 2004/0010718 (hereinafter Porras).

Claim 8 calls for "A method for detection of a new service involving an entity...retrieving a baseline list of port protocols used by a the entity being tracked...retrieving a current list of port protocols...and determining whether there is a difference in the port protocols, by having a protocol that was in a current list but was not in the baseline list; and if there is a difference; indicating a new service involving the tracked entity."

The Examiner contends that:

> **As per claim 8, Porras et al discloses a method for detection of a new service involving an entity, the method comprises: Porras et al discloses monitoring network activity of an entity (see page 1, paragraph 11) that meets the recitation of entity being tracked, which includes analyzing event records such as port protocols (see page 3, paragraph 31) the method includes collecting statistical measures that includes port protocols over a period of time comprising the most recent data represented as short-term statistical profiles (current list) and the normal, non-recent, data as long-term statistical profiles (baseline list) (see page 1, paragraphs 11 and 15, page 3, paragraphs 33 and 36 and page 4, paragraph 40) that meets the recitation of retrieving a baseline list of port protocols used by a(n) entity being tracked, the baseline value determined over a baseline period, retrieving a current list of port protocols for the entity being tracked; and further discloses a comparison is made between the two wherein the difference between them indicates suspicious network activity or abnormal activity (see page 1, paragraphs 11 and 15) or indication of new service (see page 3, paragraphs 33 and 36 and page 4, paragraph 47) that meets the recitation of determining whether there is a difference in the port protocols, by having a protocol that was in a current list but was not in the baseline list; and if there is a difference; indicating a new service involving the tracked entity. (emphasis added)**

Applicant contends that Porras neither describes nor suggests at least "...determining whether there is a difference in the port protocols, by having a protocol that was in a current list but was not in the baseline list; and if there is a difference; indicating a new service involving the tracked entity." The discussions at page 3, paragraphs 33 and 36 and page 4, paragraph 47 in

Porras do not describe or suggest these features. For example, Porras at page 3, paragraph 33 states:

> **[0033] Selection of packets can be based on different criteria. Streams of event records can be derived from discarded traffic (i.e., packets not allowed through the gate-way because they violate filtering rules), pass-through traffic (i.e., packets allowed into the internal network from external sources), packets having a common protocol (e.g., all ICMP (Internet Control Message Protocol) packets that reach the gateway), packets involving network connection management (e.g., SIN, RESET, ACK, [window resize]), and packets targeting ports to which an administrator has not assigned any network service and that also remain unblocked by the firewall. Event streams may also be based on packet source addresses (e.g., packets whose source addresses match well-known external sites such as satellite offices or have raised suspicion from other monitoring efforts) or destination addresses (e.g., packets whose destination addresses match a given internal host or workstation). Selection can also implement application-layer monitoring (e.g., packets targeting a particular network service or application). Event records can also be produced from other sources of network packet information such as report logs produced by network entities. Event streams can be of very fine granularity. For example, a different stream might be derived for commands received from different commercial web-browsers since each web-browser produces different characteristic network activity. (emphasis added)**

As shown, Porras merely describes the selection of packets based on different criteria in this paragraph. In paragraph 36, which is set forth below, Porras describes that categorical measures assume values from a discrete, non-ordered set of possibilities. Nowhere does Porras describe or suggest "...determining whether there is a difference in the port protocols, by having a protocol that was in a current list but was not in the baseline list; and if there is a difference; indicating a new service involving the tracked entity."

> **[0036] Categorical measures assume values from a discrete, nonordered set of possibilities. Examples of categorical measures include network source and destination addresses, commands (e.g., commands that control data transfer and manage network connections), protocols, error codes (e.g., privilege violations, malformed service requests, and malformed packet codes), and port identifiers. The profiler engine 22 can build empirical distributions of the category values encountered, even if the list of possible values is open-ended. The engine 22 can have mechanisms for "aging out" categories whose long-term probabilities drop below a threshold.**

In paragraph 47, Porras teaches comparing unknown port traffic with any known packet sets (e.g., FTP, Telnet, SMTP, HTTP). As such, Porras is not understood to disclose or suggest a baseline list[1]. The examiner seems to equate "know packet sets" to "baseline list."

---

[1] A baseline list as defined by Applicant is: a list of port protocols (service or ports) used by that host <host id> over a baseline period, which could be over a preceding week or so. (Specification paragraph 55)

> **[0047] Signature analysis can also scan traffic directed at unused ports (i.e., ports to which the administrator has not assigned a network service). Here, packet parsing can be used to study network traffic after some threshold volume of traffic, directed at an unused port, has been exceeded. A signature engine 24 can also employ a knowledge base of known telltale packets that are indicative of well-known network-service protocol traffic (e.g., FTP, Telnet, SMTP, HTTP). The signature engine 24 then determines whether the unknown port traffic matches any known packet sets. Such comparisons could lead to the discovery of network services that have been installed without an administrator's knowledge. (emphasis added)**

Claim 9

Claim 9 depends directly from claim 8, and requires: "determining if the entity is providing or using the new service." The examiner uses paragraph 33, 36 and 47 which are reproduced above to reject claim 9 without specifically pointing out relevant discussions in these paragraphs. However, as understood, these passages neither describe nor suggest: "determining if the entity is providing or using the new service." Applicant's claim 9 is distinct and allowable over the art.

Claims 9-14 are allowable for at least for the reasons discussed in claim 8.

Claim 15 and dependent claims 16-22 drawn to a computer program product analogue of claims 8-14, are allowable for analogous reasons as those given for claim 1 and the respective dependent claims.

35 U.S.C § 103

The examiner rejected Claims 10, 14, 17 and 22 under 35 U.S.C. 103(a), as being unpatentable over Porras U.S. Patent Publication 2004/0010718.

The Examiner argues that:

> **As per claim 10, Porras et al substantially discloses determining whether the activity exceeds a threshold value when the entity is using a new service (unknown port) and if the threshold exceeds and the entity is using a new service, anomaly is detected (see page 4, paragraph 47 and 48). Porras et al suggests using a countermeasure response to report the anomaly (see pages 6-7, paragraphs 67 and 71). Although not using the same terms as the claim language it is apparent to one of ordinary skill in the art of intrusion detection that a rule for issuing an alert may be defined as exceeding a threshold value which indicates an attack as disclosed Porras et al and producing a countermeasure response or reporting the attack in response to detecting can be reasonably interpreted as generating an alert. As known in the art, in an attack-response method when an attack is detected according to a specified rule, an alert is generated. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to issue an alert if is determined whether a rule specifies to issue an alert if the entity is providing or using the new service; and if it is also determined that the entity is providing or using the new service so as to protect the network from more global attacks by**

**taking further actions (see page 7, paragraph 68) or by alerting other entities (see page 2, paragraph 16) as suggested by Porras et al.**

However, the discussion at page 4, paragraph 47 and 48 in Porras deals with applying signature analysis to scan traffic directed at unused ports (i.e., ports to which the administrator has not assigned a network service). As such, Porras neither describe nor suggest "determining if the entity is providing or using the new service." Porras seems to apply a threshold value of traffic to a specific port to detect and report suspicious activities, rather than differentiate if the entity is providing or using a new service before issuing an alert as required by claim 10. Applicant's claim 19 is distinct and allowable over Porras. Claim 17 recites similar features in claim 10 and therefore allowable at least for the reasons given in claim 10.

In rejecting claim 14, the Examiner acknowledges in the Office Action on page 6 that: "**As per claim 14, Porras et al substantially discloses measuring network connections and using a statistical profile to make the comparison (see page 1, paragraph 1-2) but does not explicitly disclose that the statistical profile is represented as a connection table. Examiner takes official notice that it is very well known in the art that network events can be represented in a form of a table and it would have been obvious to one of ordinary skill in the art at the time the invention was made... (emphasis added)**"

Applicant requests that the Examiner provide documentary evidence to support the statement[2] that: "**it is very well known in the art that network events can be represented in a form of a table and it would have been obvious to one of ordinary skill in the art at the time the invention was made... .**"

Applicant makes a similar request regarding claim 22, that the Examiner provide documentary support of "...**official notice that it is very well known in the art that network events can represented in a form of a table and it would have been obvious to one of ordinary skill in the art at the time the invention was made...**"

35 U.S.C § 103

The examiner rejected Claims 1-7 under 35 U.S.C. 103(a), as being unpatentable over Porras in view of Cooper, U.S. Patent 7,047,288.

Claim 1 calls for "A graphical user interface for configuring a new service detection process...comprising: a first field that depicts choices for entities to track in the network; a

[2] MPEP 2144.03 states that "if applicant challenges a factual assertion as not properly officially noticed or not properly based upon common knowledge, the examiner must support the finding with adequate evidence ... If applicant adequately traverses the examiner's assertion of official notice, the examiner must provide documentary evidence in the next office action if the rejection is to be maintained.

second field that allows a system to track if the selected entity is providing or consuming a service; a third field that depicts a range over which to track an entity selected in the first field; and a fourth field to specify a severity for an alert generated if a new service is detected."

The Examiner argues that:

> **As per claim 1, Porras et al substantially discloses a graphical user interface (see page 3, paragraph 31) for configuring a new service detection process, and discloses tracking an entity in the network (see page 1, paragraph 11) a method that allows a system to track if the selected entity is providing or consuming a service (such as using unknown port protocol) (see pages 4-5, paragraphs 40-41, 47-48); depicts a range over which to track the selected entity (see page 3, paragraph 35); specifying severity for an alert generated if a new service is detected (see pages 4-5, paragraphs 41, and 47-48; and pages 6-7, paragraph 67). Porras et al does not explicitly disclose the details of the graphical user interface. However, it would have only required routine skill in the art to implement the step above into fields in a graphical user interface to make it interactive. Cooper et al in an analogous art teaches generating a human readable English language description of a formal specification of network security policy that allows non-technical user within a user's organization to comprehend the policy by making the description simple enough to understood (see abstract). Cooper et al discloses a graphical user interface (see for instance fig. 9) that includes several fields including field for specifying a host name, field for service being tracked (see figs. 9 and 31) that meets the recitation of a first field that depicts choices for entities to track in the network, field for specifying a range of the entity being tracked (see column 13, lines 25-67 and fig. 9) and field specifying a severity for an alert generated (see fig. 9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was make to modify Porras et al to implement the method disclosed by Porras et al into a graphical user interface represented by fields as disclosed in Cooper et al. One of ordinary skill in the art would have been recognized the advantages disclosed by Cooper et al who teaches generating a human readable English language description of a formal specification of network security policy that allows non-technical user within a user's organization to comprehend the policy by making the description simple enough to understood (see abstract).**

The Examiner acknowledges that Porras does not explicitly disclose the details of the graphical user interface, but relies on Cooper to teach all the elements of claim 1.

However, Fig. 9 (reproduced below) in Cooper shows a queried rule view dialog box. In particular, it shows that the null.spw policy has denied all traffic (col. 12 lines 1-8). However, Fig. 9 and its corresponding descriptions in Cooper does not describe "a third field that depicts a range over which to track an entity selected in the first field." The selections of "Final Rule Name" and "Disposition Name" from respective pull down menus in Fig. 9 merely offer the user the range for policy rules that can be applied and policy of what action or state change needs to take place in response to a network event (see col. Table A terminologies of Rule and Disposition).

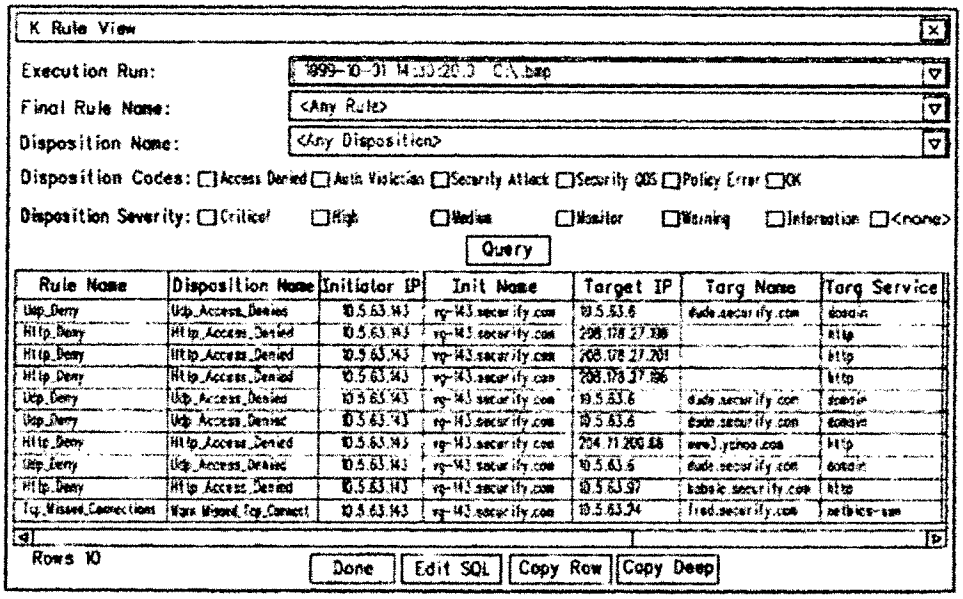


*FIG. 9*

The Examiner also argues that the discussion at col. 13 lines 25-67 discloses that "a third field that depicts a range over which to track an entity selected in the first field." Applicant disagrees. In contrast, this portion of discussion refers to Fig. 11 which shows a high-level view of an example network. However, that discussion does not concern a graphical user interface for configuring a new service detection process (see reproduced Fig. 11 below), and the discussion is silent with regard to "a third field that depicts a range over which to track an entity selected in the first field."

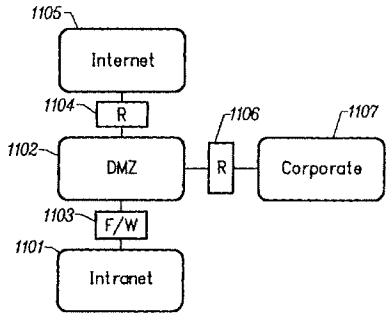


*FIG. 11*

Applicant's claim 1 is distinct and allowable over Porras in view of Cooper.

Claims 2-7 are allowable at least for the reasons discussed in claim 1.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Any circumstance in which the applicants have (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

In view of the foregoing, applicants respectfully request entry of the amendment since it addresses specific objections first raised by the examiner in the instant office action, does not require any further consideration or search. Accordingly, applicants submit that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date:March 4, 2008

/Denis G. Maloney/
Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906